

GARCIA THIERRY
2eme Année de BTS SIO ICOGES LYON
Option SISR
thierry.garcia0404@gmail.com

---

pfSense

Manuel d’Installation et d’Utilisation du Logiciel



1. Installation de pfSense :

Téléchargez l'image de pfSense dans la section « Download » de pfSense (http://www.pfsense.com)

Démarrez votre ordinateur à partir du cd de l'image de pfSense ; l'installation va alors commencer.

Laissez alors le compte à rebours se terminer (10 secondes) ou appuyez directement sur « Entrée ». Le démarrage par défaut est choisit.



Ensuite vient la configuration des interfaces réseaux.

FreeBSD détecte le nombre de cartes réseaux, et y attribue des noms .

```
Valid interfaces are:

le0     00:0c:29:ce:ba:bd
le1     00:0c:29:ce:ba:c7
le2     00:0c:29:ce:ba:d1
```

Nous allons à présent choisir quelle interface appartient au LAN, au WAN Il suffit alors de renseigner son nom.
Pour connaître avec certitude la carte réseau que l'on affecte, il est possible de faire de l'auto détection, c'est à dire que lorsqu'une carte réseau est branchée, elle devient « UP ».

```
If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: le0

Enter the WAN interface name or 'a' for auto-detection: le1

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished): le2

Enter the Optional 2 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

LAN  -> le0
WAN  -> le1
OPT1 -> le2

Do you want to proceed [y|n]? y
```

Une fois les interfaces assignées, nous arrivons enfin au menu.

```
  LAN*                       ->   le0      ->      192.168.1.1
  WAN*                       ->   le1      ->      0.0.0.0(DHCP)
  OPT1(OPT1)                 ->   le2      ->      NONE

 pfSense console setup
***********************
 0)  Logout (SSH only)
 1)  Assign Interfaces
 2)  Set LAN IP address
 3)  Reset webConfigurator password
 4)  Reset to factory defaults
 5)  Reboot system
 6)  Halt system
 7)  Ping host
 8)  Shell
 9)  PFtop
10)  Filter Logs
11)  Restart webConfigurator
12)  pfSense PHP shell
13)  Upgrade from console
99)  Install pfSense to a hard drive/memory drive, etc.

Enter an option:
```

Nous voilà de nouveau au menu. Nous allons à présent installer réellement pfSense sur le disque dur. Saisir alors le choix « 99 ».

```
Enter an option: 99
```

L'installation qui va suivre se fait en acceptant toutes les options par défaut. Il suffit d'accepter toutes les demandes (formatage si nécessaire et création de la partition).




```
Select Task

Choose one of the following tasks to
perform.

< Install pfSense >
< Reboot >
< Exit >
```

On choisit d’installer pfSense.

```
Select a Disk

Select a disk on which to install pfSense.

< ad0: 2048MB <VMware Virtual IDE Hard Drive 00000001> at ata0-master U >
< Return to Select Task >
```

On sélectionne le disque dur dans lequel sera installé pfSense.

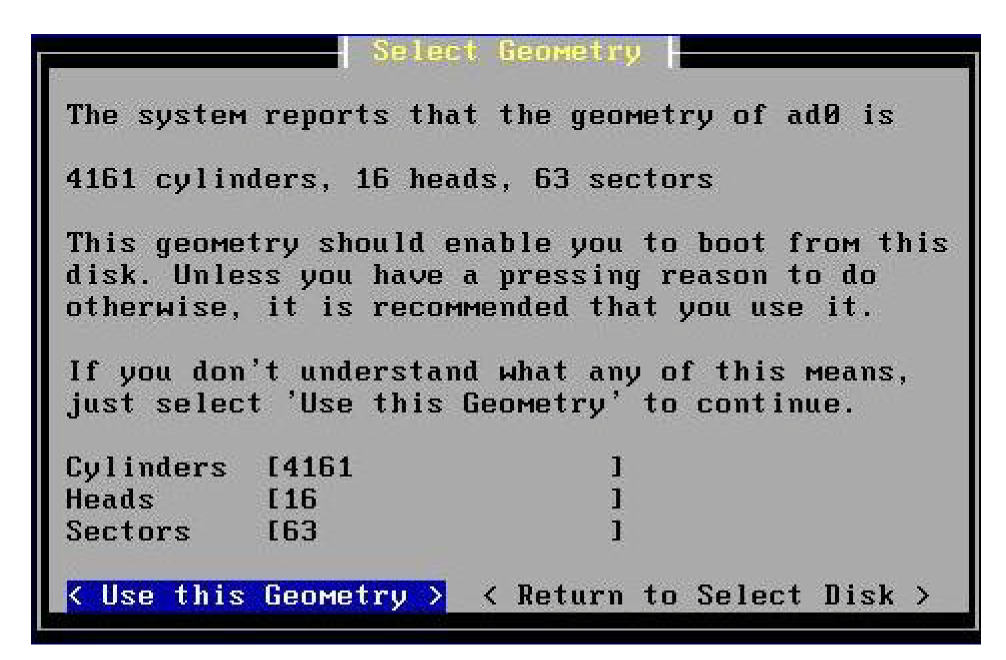
```
Format this Disk?

Would you like to format this disk?

You should format the disk if it is new, or if you wish to start
from a clean slate. You should NOT format the disk if it contains
information that you want to keep.

< Format this Disk >  < Skip this step >
< Return to Select Disk >
```

Si nécessaire, sélectionnez l’option « Format this Disk ». C’est cela dit plus prudent de formater le disque dur même s’il est censé être vide.



Ici on peut modifier la géométrie du disque dur. Cette étape n'est en principe pas nécessaire. En effet, FreeBSD reconnaît quasiment tous les disques durs existants. A ne changer donc uniquement si le disque est trop récent et donc pas reconnu.

ABOUT TO FORMAT! Proceed?

WARNING! ALL data in ALL partitions on the disk

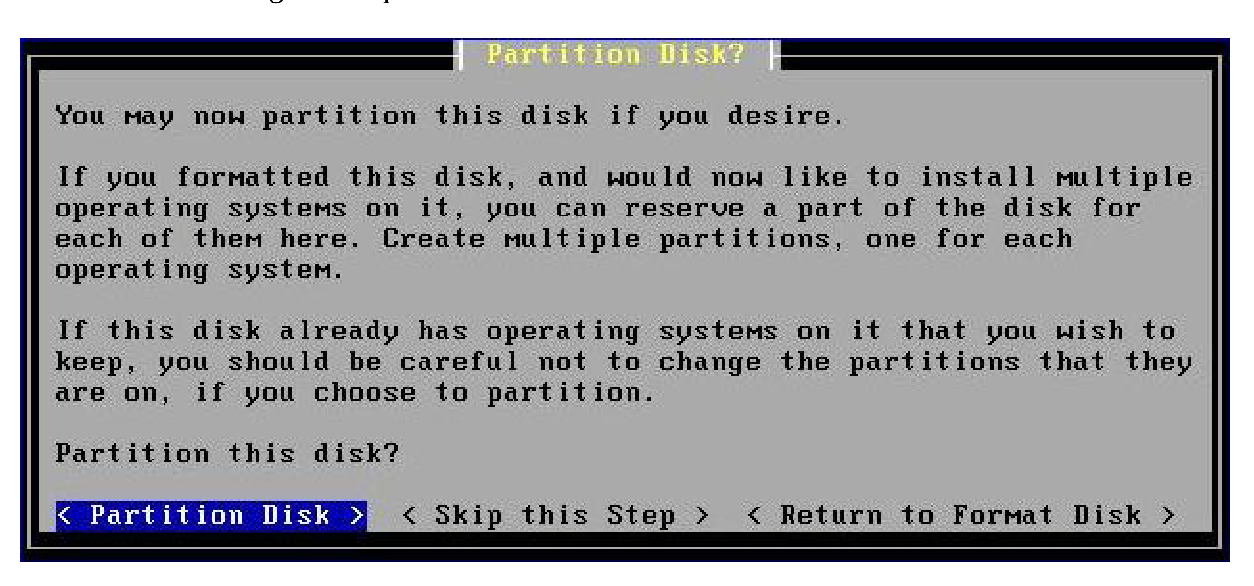
ad0: 2048MB <VMware Virtual IDE Hard Drive 00000001> at ata0-master UDMA33

will be IRREVOCABLY ERASED!

Are you ABSOLUTELY SURE you wish to take this action? This is your LAST CHANCE to cancel!

< Format ad0 > < Return to Select Disk >

Confirmez le formatage du disque dur.



Nous allons maintenant créer les partitions sur le disque dur. Nous pouvons créer autant de partitions que nous le souhaitons dans le cas où plusieurs systèmes d'exploitations seraient mis en place.

Edit Partitions

Select the partitions (also known as 'slices' in BSD tradition) you want to have on this disk.

For Size, enter a raw size in sectors (1 gigabyte = 2097152 sectors) or a single '*' to indicate 'use the remaining space on the disk'.

Size (in Sectors) Partition Type Active?
[4194225] [FreeBSD] [X] < Ins > < Del >
< Add >

< Accept and Create > < Return to Format Disk >
< Revert to Partitions on Disk >

Vous pouvez ici soit garder la taille de la partition (par défaut il utilisera tout le disque dur) ou lui définir une taille.

```
Partition Anyway?

No changes appear to have been made to the partition table layout.

Do you want to execute the commands to partition the disk anyway?

< Yes, partition ad0 >  < No, Skip to Next Step >
        < No, Return to Edit Partitions >
```

Confirmez la création de la partition.



Sélectionnez à présent la partition où vous allez installer pfSense.



Ce message averti seulement que les données existantes sur la partition vont être écrasées.

```
Select Subpartitions

Set up the subpartitions (also known as just 'partitions' in BSD tradition)
you want to have on this primary partition.

For Capacity, use 'M' to indicate megabytes, 'G' to indicate gigabytes, or a
single '*' to indicate 'use the remaining space on the primary partition'.

Mountpoint   Capacity
[/         ] [*       ] < Ins > < Del >
[swap      ] [256M    ] < Ins > < Del >
                        < Add >

      < Accept and Create >  < Return to Select Partition >
                   < Switch to Expert Mode >
                      Press F1 for Help
```

Sur tout système Linux, il existe une partition swap (partition d'échange). C'est un espace réservé pour « rajouter » de la mémoire. La taille de la partition swap dépend généralement de la RAM présente sur l'ordinateur.

```
Install Kernel(s)

You may now wish to install a custom kernel configuration.

< Uniprocessor kernel (one processor) >
< Symmetric multiprocessing kernel (more than one processor) >
< Embedded kernel (no vga console, keyboard >
< Developers kernel (includes GDB, etc) >
Press F1 for Help
```

Sélectionnez le type du kernel (noyau) à installer.

```
Install Bootblock(s)

You may now wish to install bootblocks on one or more disks. If you already
have a boot manager installed, you can skip this step (but you may have to
configure your boot manager separately.) If you wish to install pfSense on a
disk other than your first disk, you will need to put the bootblock on at
least your first disk and the pfSense disk.

Disk Drive   Install Bootblock?   Packet mode?   Use Grub
[ad0      ]  [X]                  [ ]            [ ]

< Accept and Install Bootblocks >  < Skip this Step >
< Return to Install Kernel >
Press F1 for Help
```

Nous allons maintenant créer le « boot » du disque dur. Cela va permettre de démarrer la machine directement sur pfSense.



Si pfSense s'est installé correctement, vous pouvez retirer le cd et redémarrer la machine en allant sur « reboot ».

2. Configuration de pfSense :

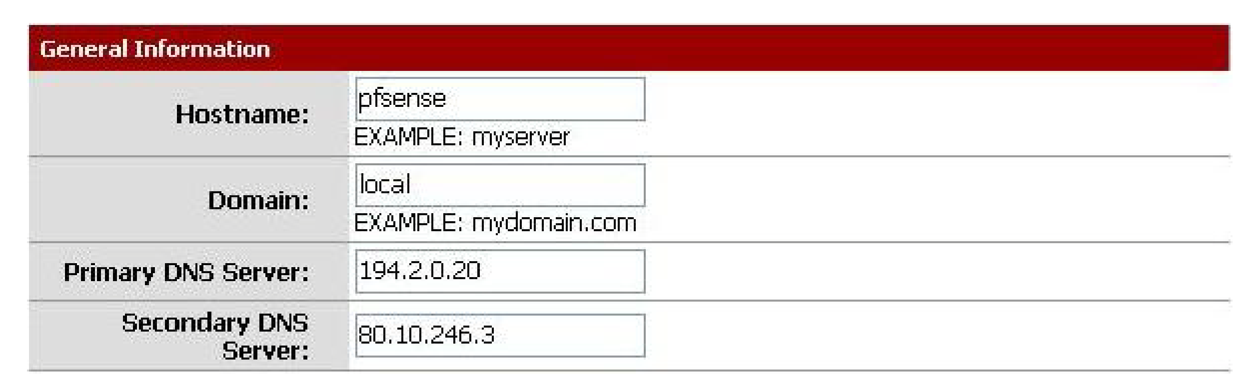
PfSense est désormais disponible à l'adresse du LAN : http://192.168.100.1

→ login : admin ; mdp : pfsense (par défaut)

C'est à partir de cette adresse que toutes les manipulations vont se dérouler.

2.2 Préparation de la configuration :

Lors de la connexion à l'adresse de pfSense, une aide à la configuration apparaît. Elle permet de configurer la base de pfSense. Il est conseillé de l'utiliser même si par la suite les informations renseignées peuvent être changées.



Dans notre cas, nous renseignons les DNS primaires des deux connexions.



Ce logiciel utilise le protocole NTP (Network Time Protocol) qui permet de synchroniser les horloges des systèmes informatiques à travers un réseau dont la latence est variable.

Configure WAN Interface	
SelectedType:	Static

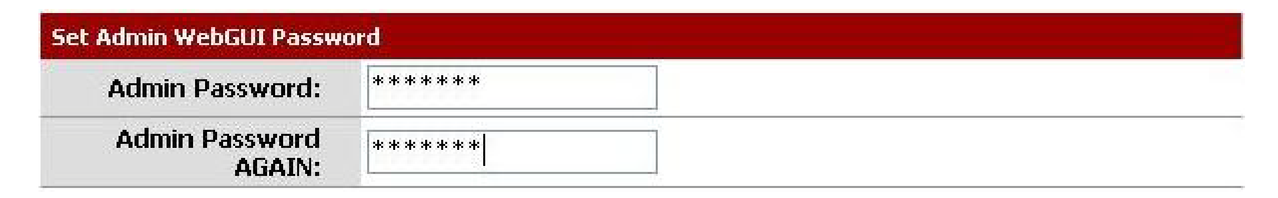
General configuration	
MAC Address:	00:0c:29:ce:ba:c7 This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU:	If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

Static IP Configuration	
IP Address:	192.168.1.1 / 24

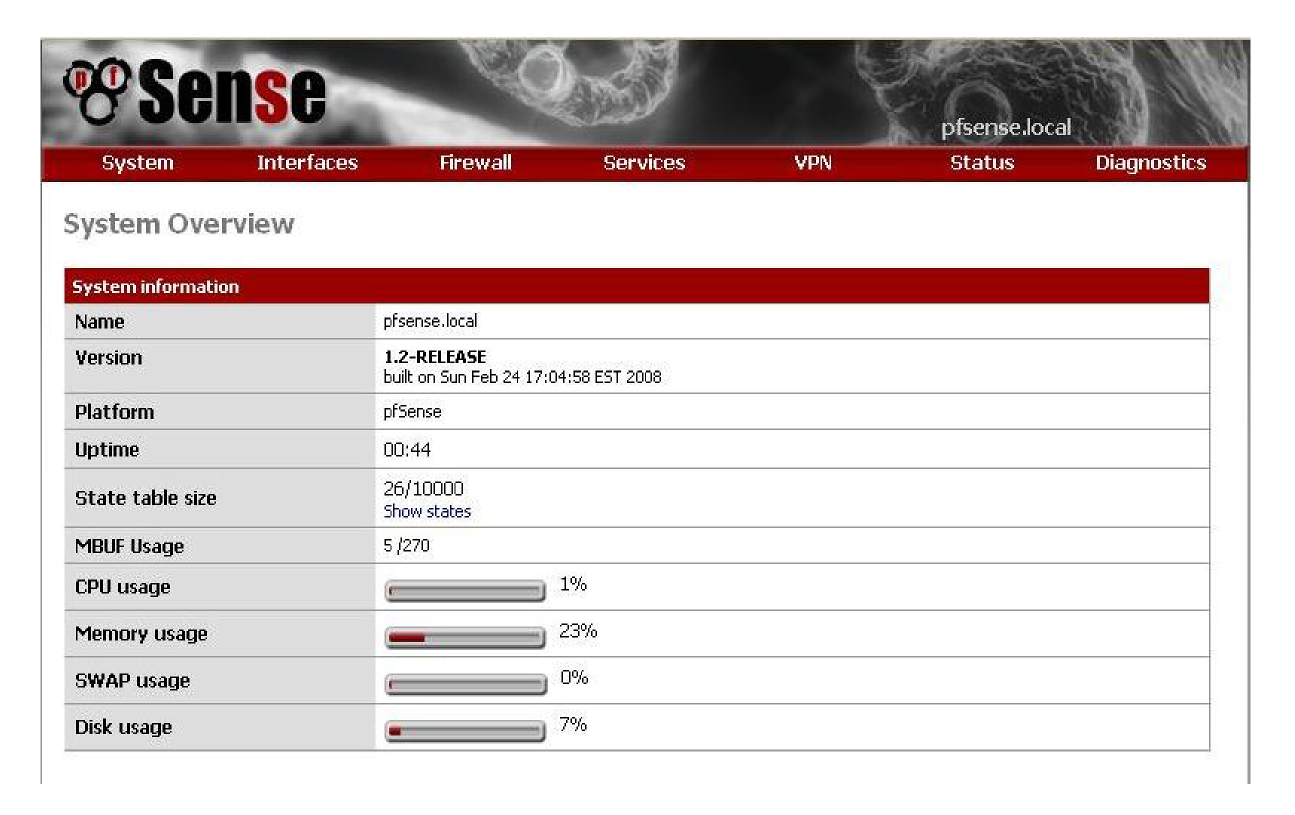
RFC1918 Networks	
Block RFC1918 Private Networks:	Block private networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

Ceci correspond à la configuration de l'interface WAN. Pour être sûr d'utiliser la bonne carte réseau, il est conseillé d'y rentrer son adresse MAC. Il ne faut également pas oublier de décocher la case « Block private networks from entering via WAN ».

Ensuite, en ce qui concerne l'interface LAN, il faut simplement s'assurer de la bonne adresse et du bon masque de sous-réseau.



Enfin, le mot de passe d'accès à l'interface graphique de pfSense est à modifier. Cela permettra de restreindre l'accès à cette interface qui doit être confidentielle.



Nous voilà enfin sur la page par défaut d'administration de pfSense.

2.3 Mise en place de la configuration de pfSense :

1.1.1. System :

Advanced :

Cette section représente les options avancées de pfSense comme l'accès SSH, les clés SSL, etc. Pour la réalisation du projet, les sticky connections (connexions persistantes) ont été acceptées.



Cette option permet d'éviter la renégociation inutile des clés SSL pour le protocole HTTPS.

Firmware :

Cela permet de mettre à jour pfSense.

General Setup :

Ce sont les configurations de base de pfSense rentrées lors du guide d'installation. Il faut vérifier que « Allow DNS server list to be overridden by DHCP/PPP on WAN » est bien décoché.

DNS servers	194.2.0.20 80.10.246.3 IP addresses; these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients ☐ **Allow DNS server list to be overridden by DHCP/PPP on WAN** If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). They will not be assigned to DHCP and PPTP VPN clients, though.

Packages :

Il est possible d'installer de nouveaux paquets tels que MRTG (interface graphique à SNMP), Squid (serveur mandataire), etc.

Setup Wizard :

Le Setup Wizard est le guide rencontré au début de l'installation de pfSense. Il est possible de le refaire.

Static Route :

Les routes statiques sont importantes lorsqu'une adresse réseau n'est pas « vue » par la passerelle.

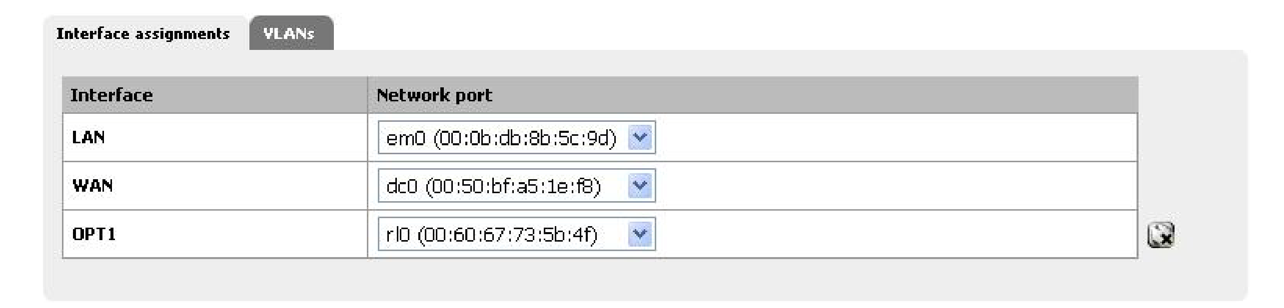
Interface	Network	Gateway	Description
OPT1	80.10.246.3/32	192.168.2.254	

L'interface WAN est notre interface par défaut. OPT1 n'est pas forcément utilisée et va pointer vers l'interface WAN (ce qu'on ne veut pas). Il est alors judicieux d'ajouter une route statique pour le DNS.

1.1.2. Interfaces :

(assign) :

Il est possible de modifier l'attribution d'une interface à une carte réseau à l'aide de l'adresse MAC. Les VLANs peuvent également y être gérés.



WAN :

Cette interface a été configurée lors du guide d'installation de pfSense.

LAN :

Celle-ci a également été configurée dans le guide d'installation de pfSense.

OPT1 :

Cette interface correspond à notre liaison de secours. Elle porte le nom de « Optional 1 » (OPT1). Sa configuration est proche de celle de l'interface WAN.

Optional Interface Configuration

	☑ **Enable Optional 1 interface**
Description	OPT1 Enter a description (name) for the interface here.

General configuration

Type	Static
MAC address	00:60:67:73:5b:4f Copy my MAC address This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

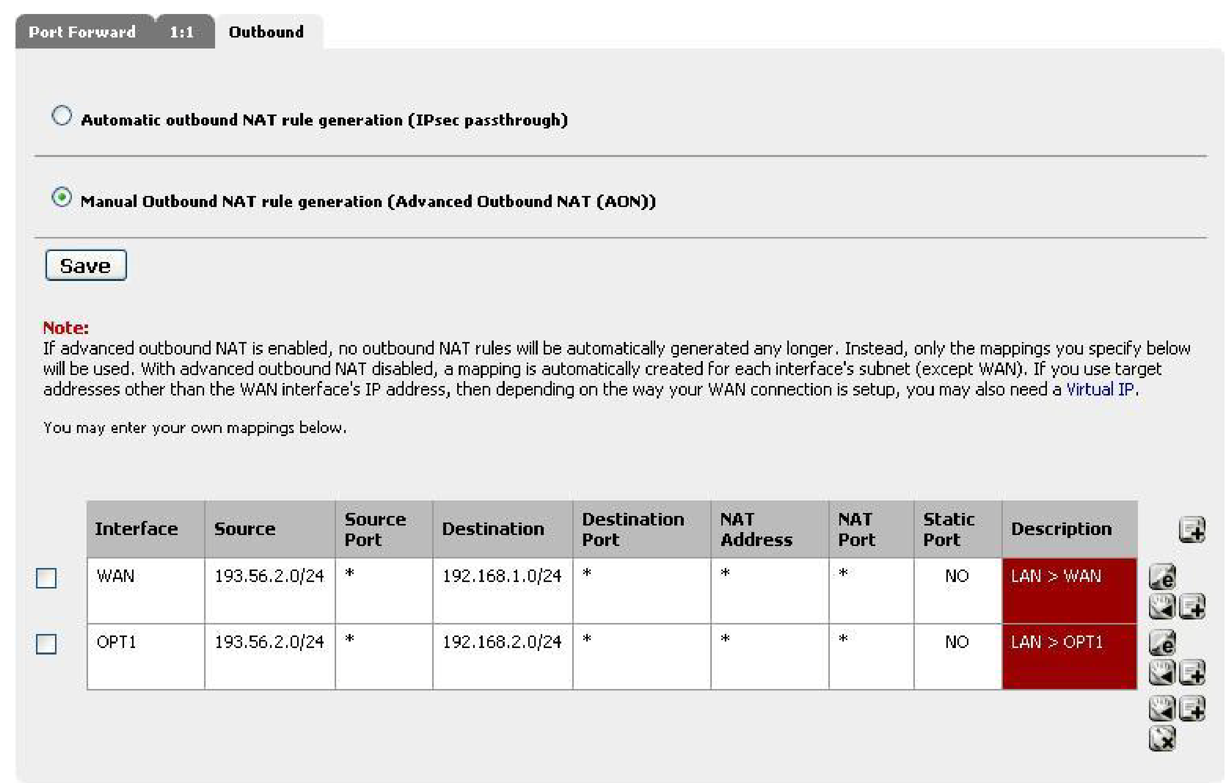
1.1.3. Firewall :

Aliases :

Les alias permettent principalement d'associer un nom à une adresse d'hôte, un port, ou un réseau. Un nom peut comprendre plusieurs éléments, ce qui facilite et simplifie les règles à appliquer aux hôtes spécifiés.

NAT :

Le NAT (Network Address Translation) permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé.
Dans notre cas, le NAT sera utilisé pour les deux connexions Internet.



Rules :

<u>Règle par défaut : Tout est bloqué.</u> Elle n’est pas explicitement écrite mais est appliquée.

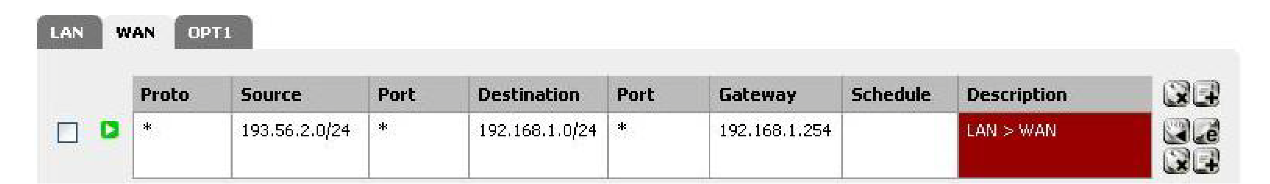
LAN :

LAN | WAN | OPT1

Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
*	LAN net	*	172.30.3.0/24	*	192.168.2.254		LAN > VPN LARRIEUX via OPT1
*	LAN net	*	192.168.2.0/24	*	192.168.2.254		LAN > Réseau OPT1
*	LAN net	*	192.168.1.0/24	*	192.168.1.254		LAN > Réseau WAN
*	LAN net	*	*	*	FailOver		LAN > Internet (WAN ou OPT1)

La passerelle « FailOver » correspond au changement de connexion en cas de crash (vu dans la partie « Services »).

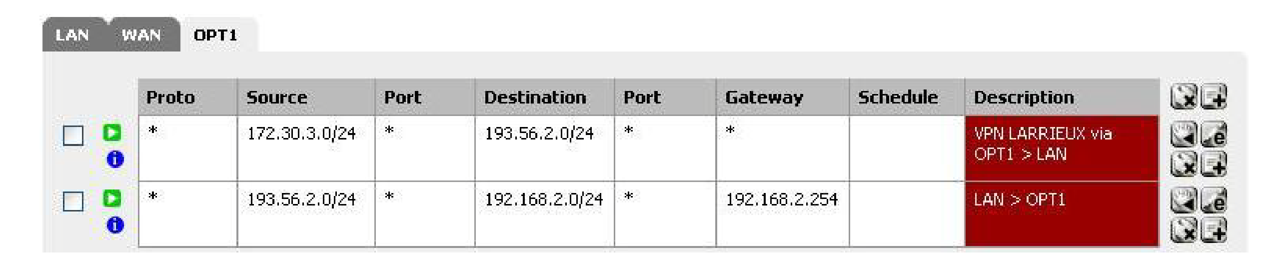
WAN :



LAN | WAN | OPT1

Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
*	193.56.2.0/24	*	192.168.1.0/24	*	192.168.1.254		LAN > WAN

OPT1 :



LAN | WAN | OPT1

Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
*	172.30.3.0/24	*	193.56.2.0/24	*	*		VPN LARRIEUX via OPT1 > LAN
*	193.56.2.0/24	*	192.168.2.0/24	*	192.168.2.254		LAN > OPT1

Schedules :

Schedule (planifier) correspond à un intervale de temps dans le mois ou dans la journée. Ces planifications sont à attribuer à des règles de Firewall. Ces règles sont alors actives en fonction d’une plage d’horaire précise. Par exemple, l’accès Internet ne sera autorisé que de 9h à 19h.

Traffic Shaper :

Le Traffic Shaping permet de contrôler l’utilisation de la bande passante. On peut par exemple limiter la bande passante d’un hôte ou d’un port. Cependant, le Traffic Shaping ne peut être réalisé qu’avec une seule interface Internet et non deux comme dans notre cas. Nous ne pourrons donc pas l’utiliser correctement. On peut toutefois l’activer sur une des deux interfaces.

Virtual IPs :

Il est possible d'assigner des adresses IP virtuelles. Ceci permet d'avoir un hôte avec plusieurs adresses IP.
Dans cette partie, on peut aussi configurer le CARP (Common Address Redundancy Protocol).
L'objectif premier de ce protocole est de permettre à un groupe d'hôtes sur un même segment réseau de partager une adresse IP.
L'utilisation principale de CARP est la création d'un groupe de pare-feu redondants. L'adresse IP virtuelle attribuée au groupe de redondance est désignée comme l'adresse du routeur par défaut sur les machines clientes. Dans le cas où le pare-feu maître rencontrerait une panne ou est déconnecté du réseau, l'adresse IP virtuelle sera prise par un des pare-feu esclaves et le service continuera à être rendu sans interruption.

1.1.4. Services :

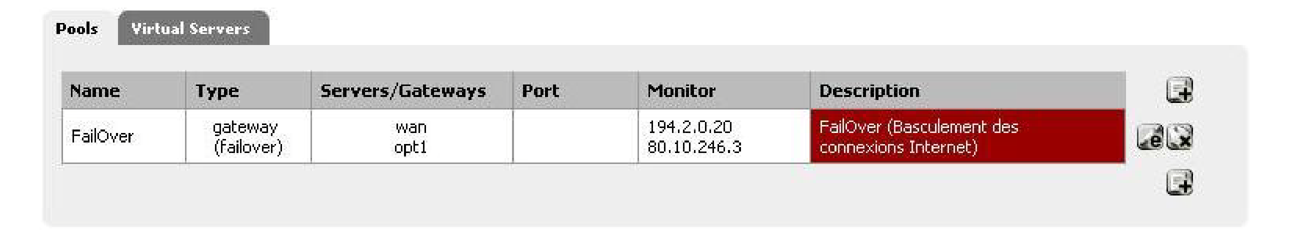
Plusieurs services peuvent être gérés par pfSense. Ils peuvent être arrêtés ou activés depuis cette interface.

Voici la liste des services :

- **Captive Portal** (portail captif)
- **DNS Forwarder** (transporte les DNS)
- **DHCP relay** (agent relais DHCP)
- **DHCP server** (serveur DHCP)
- **Dynamic DNS** (permet de rendre « statique » un DNS dynamique grâce à un nom)
- **Load Balancer** (répartition de charges)
- **OLSR** (protocole de routage)
- **PPPoE server** (permet de bénéficier des avantages de PPP sur Ethernet)
- **RIP** (protocole de routage)
- **SNMP** (gérer des équipements réseaux à distance)
- **UpnP** (facilite la mise en réseau)
- **OpenNTPD** (gestion de l'horloge)
- **Wake on LAN** (permet à un ordinateur éteint d'être démarré à distance)

Nous ne nous intéresserons qu'au service **Load Balancer**. C'est celui-ci qui nous permettra de configurer le FailOver et donc la redondance des connexions Internet.

Le principe du FailOver est d'utiliser le protocole ICMP afin de « pinguer » une passerelle (le DNS étant l'idéal pour savoir si une connexion Internet fonctionne ou non). Notre passerelle principale est Internet1 (WAN) et la passerelle de secours correspond à Internet2 (OPT1). Si le ping vers la passerelle du WAN ne fonctionne plus, la connexion est alors dirigée vers OPT1. Puis lorsque la passerelle WAN redevient active, la connexion est ramenée à sa passerelle par défaut (WAN). Pour utiliser correctement cette fonctionnalité, il nous faut créer le pool d'adresses ci-après.


Pools | Virtual Servers

Name	Type	Servers/Gateways	Port	Monitor	Description
FailOver	gateway (failover)	wan opt1		194.2.0.20 80.10.246.3	FailOver (Basculement des connexions Internet)

1.1.5. VPN :

Plusieurs catégories de VPN sont supportées par pfSense.

Le VPN IPSec peut être utilisé en mode transport (hôte à réseau ou hôte à hôte) ou en mode tunnel (réseau à réseau). Il sait gérer le protocole AH (Authentification) et ESP (Cryptage). Il gère également les autorités de certification.

Le VPN OpenVPN gère les serveurs et les clients VPN. Il gère également les autorités de certification.

Le VPN PPTP gère aussi les serveurs et les clients. Il prend en compte un serveur RADIUS pour l'authentification. Du côté client, un simple login/mot de passe est à renseigner.

1.1.6. Status :

L'onglet Status permet de voir l'état de pfSense. Nous pouvons par exemple vérifier si les interfaces sont actives, leurs adresses, etc.
Cela dit, quelques « status » sont plus importants que d'autres : **Interfaces** pour voir l'état des connexions ; **Load Balancer** pour vérifier si le FailOver fonctionne ; **Services** pour arrêter ou lancer un service ; **System** qui est la page d'accueil et nous permet de voir l'état du système ; et pour finir, le plus important : **System Logs** qui sont les logs de tous les services.

1.1.7. Diagnostics :

Ceci correspond à quelques fonctionnalités supplémentaires servant à rendre quasi-complète l'administration du serveur à distance. Nous pouvons donc arrêter ou redémarrer pfSense, visualiser la table de routage, effectuer un « ping », modifier des fichiers, revenir à une installation de pfSense neuve, etc.